SF 86
Questionaire For National Security Positions

SF 328
Certificate Pertaining to Foreign Interests

Appendix B
Sample Acceptable Use Policy

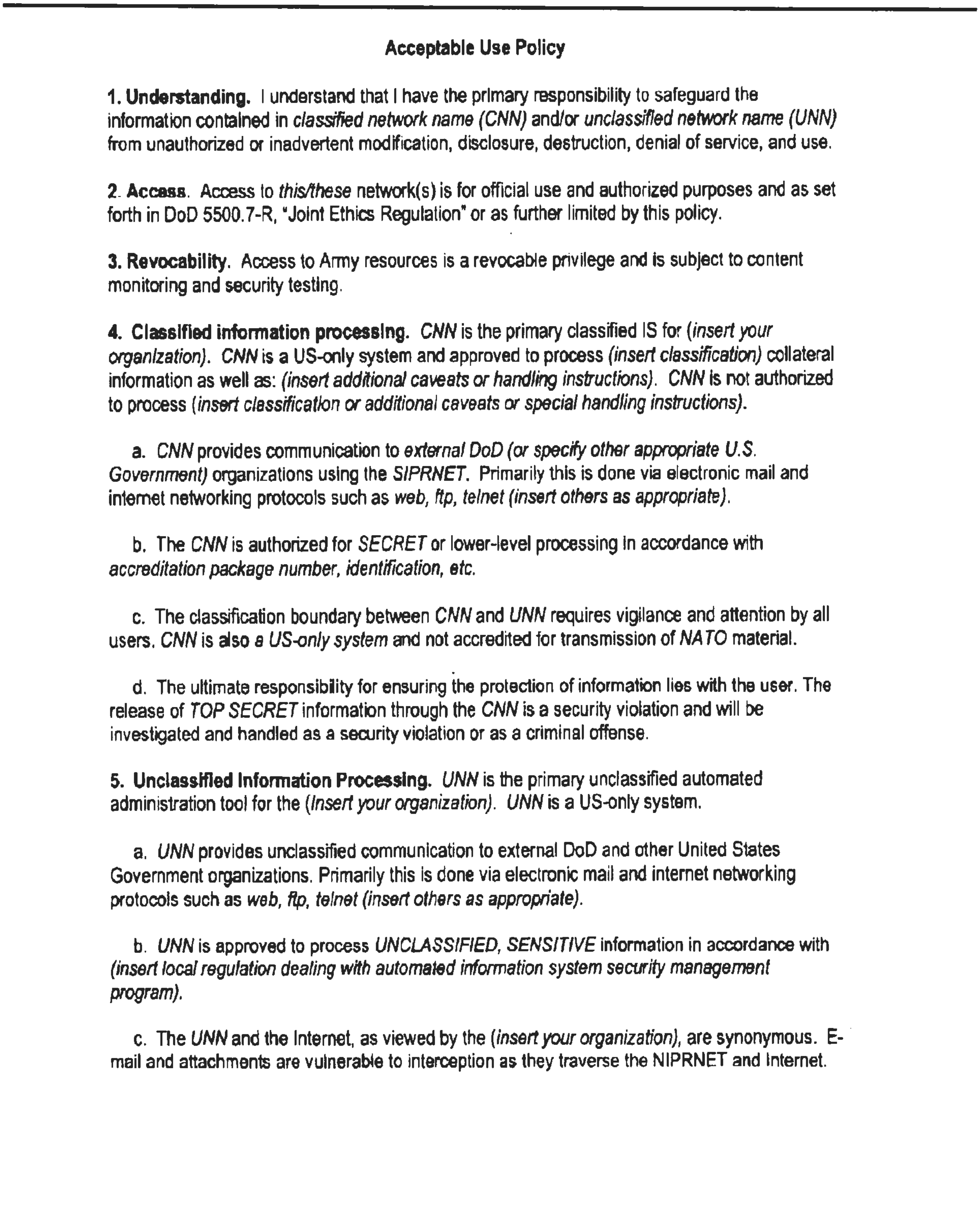
B–1. Purpose

This appendix provides a sample AUP that may be used by organizations to obtain explicit acknowledgements from individuals on their responsibilities and limitations in using ISs.

B–2. Explanation of conventions in sample acceptable use policy

Figure B–1, below, illustrates a representative AUP. In this figure, text appearing in italicized font should be replaced with the appropriate information pertinent to the specific AUP being executed. Army organizations may tailor the information in the sample AUP to meet their specific needs, as appropriate.

PROSECUTION EXHIBIT 94 for identification
PAGE OFFERED:____PAGE ADMITTED:____
PAGE 1 OF 4 PAGES



Acceptable Use Policy

1. **Understanding.** I understand that I have the primary responsibility to safeguard the information contained in *classified network name (CNN)* and/or *unclassified network name (UNN)* from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use.

2. **Access**. Access to *this/these* network(s) is for official use and authorized purposes and as set forth in DoD 5500.7-R, "Joint Ethics Regulation" or as further limited by this policy.

3. **Revocability.** Access to Army resources is a revocable privilege and is subject to content monitoring and security testing.

4. **Classified information processing.** *CNN* is the primary classified IS for (*insert your organization). CNN* is a US-only system and approved to process *(insert classification)* collateral information as well as: *(insert additional caveats or handling instructions). CNN* is not authorized to process (*insert classification or additional caveats or special handling instructions).*

a. *CNN* provides communication to *external DoD (or specify other appropriate U.S. Government)* organizations using the *SIPRNET.* Primarily this is done via electronic mail and internet networking protocols such as *web, ftp, telnet (insert others as appropriate).*

b. The *CNN* is authorized for *SECRET* or lower-level processing in accordance with *accreditation package number, identification, etc.*

c. The classification boundary between *CNN* and *UNN* requires vigilance and attention by all users. *CNN* is also *a US-only system* and not accredited for transmission of *NATO* material.

d. The ultimate responsibility for ensuring the protection of information lies with the user. The release of *TOP SECRET* information through the *CNN* is a security violation and will be investigated and handled as a security violation or as a criminal offense.

5. **Unclassified Information Processing.** *UNN* is the primary unclassified automated administration tool for the (*Insert your organization). UNN* is a US-only system.

a. *UNN* provides unclassified communication to external DoD and other United States Government organizations. Primarily this is done via electronic mail and internet networking protocols such as *web, ftp, telnet (insert others as appropriate).*

b. *UNN* is approved to process *UNCLASSIFIED, SENSITIVE* information in accordance with *(insert local regulation dealing with automated information system security management program).*

c. The *UNN* and the Internet, as viewed by the (*insert your organization),* are synonymous. E-mail and attachments are vulnerable to interception as they traverse the NIPRNET and Internet.

Figure B–1. Acceptable use policy

6. **Minimum security rules and requirements.** As a *CNN* and/or *UNN* system user, the following minimum security rules and requirements apply:

a. Personnel are not permitted access to *CNN* and *UNN* unless in complete compliance with the (insert your organization) personnel security requirement for operating in a TOP SECRET system-high environment.

b. I have completed the user security awareness-training module. I will participate in all training programs as required (inclusive of threat identification, physical security, acceptable use policies, malicious content and logic identification, and non-standard threats such as social engineering) before receiving system access.

c. I will generate, store, and protect passwords or pass-phrases. Passwords will consist of at least 10 characters with 2 each of uppercase and lowercase letters, numbers, and special characters. I am the only authorized user of this account. (I will not use user ID, common names, birthdays, phone numbers, military acronyms, call signs, or dictionary words as passwords or pass-phrases.)

d. I will use only authorized hardware and software. I will not install or use any personally owned hardware, software, shareware, or public domain software.

e. I will use virus-checking procedures before uploading or accessing information from any system, diskette, attachment, or compact disk.

f. I will not attempt to access or process data exceeding the authorized IS classification level.

g. I will not alter, change, configure, or use operating systems or programs, except as specifically authorized.

h. I will not introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files) without authorization, nor will I write malicious code.

i. I will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the IS and will not disseminate it to anyone without a specific need to know.

j. I will not utilize Army- or DoD-provided ISs for commercial financial gain or illegal activities.

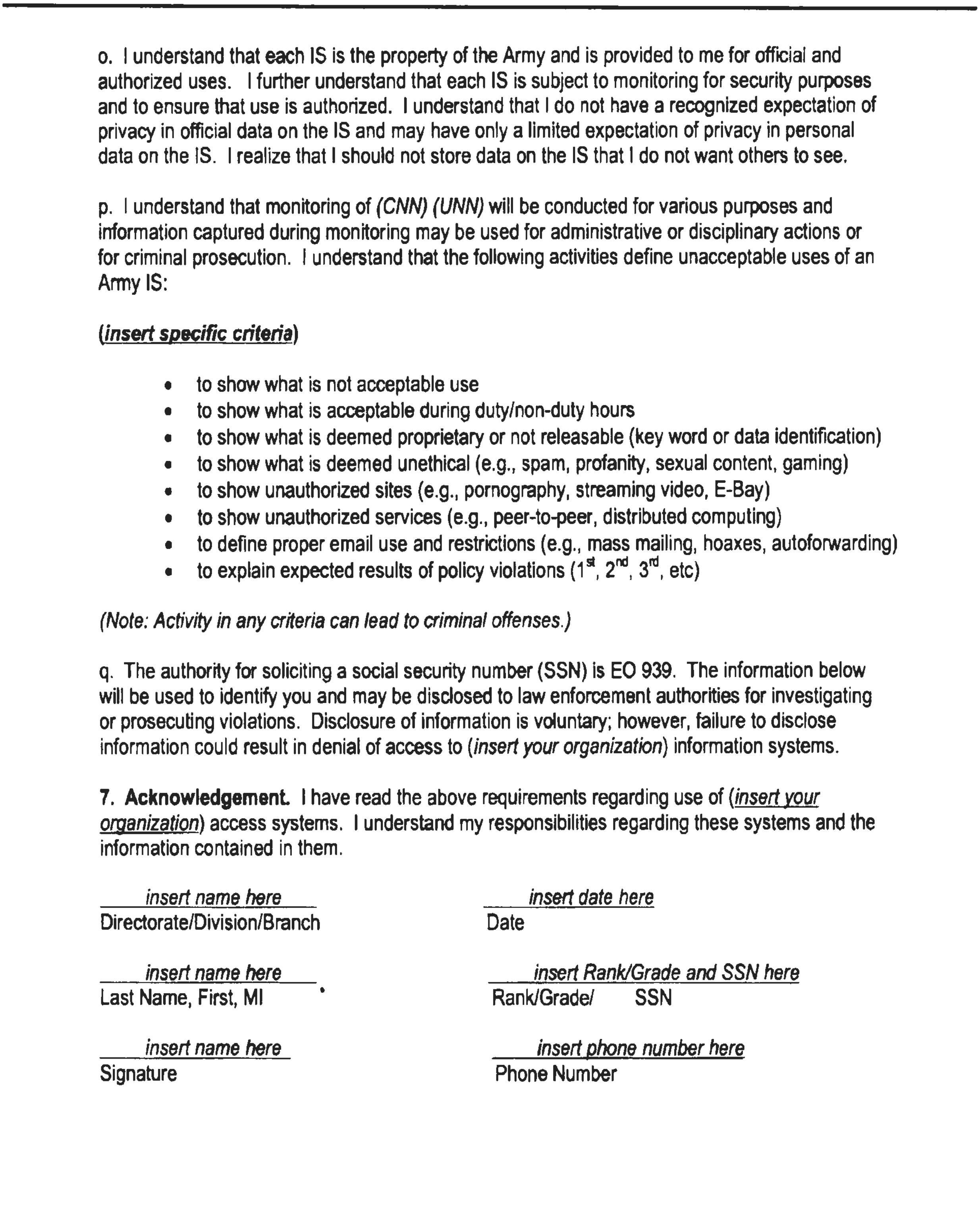
k. Maintenance will be performed by the System Administrator (SA) only.

l. I will use screen locks and log off the workstation when departing the area.

m. I will immediately report any suspicious output, files, shortcuts, or system problems to the *(insert your organization)* SA and/or IASO and cease all activities on the system.

n. I will address any questions regarding policy, responsibilities, and duties to *(insert your organization)* SA and/or IASO.

Figure B–1. Acceptable use policy—Continued



o. I understand that each IS is the property of the Army and is provided to me for official and authorized uses. I further understand that each IS is subject to monitoring for security purposes and to ensure that use is authorized. I understand that I do not have a recognized expectation of privacy in official data on the IS and may have only a limited expectation of privacy in personal data on the IS. I realize that I should not store data on the IS that I do not want others to see.

p. I understand that monitoring of *(CNN) (UNN)* will be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution. I understand that the following activities define unacceptable uses of an Army IS:

(***insert specific criteria***)

- to show what is not acceptable use
- to show what is acceptable during duty/non-duty hours
- to show what is deemed proprietary or not releasable (key word or data identification)
- to show what is deemed unethical (e.g., spam, profanity, sexual content, gaming)
- to show unauthorized sites (e.g., pornography, streaming video, E-Bay)
- to show unauthorized services (e.g., peer-to-peer, distributed computing)
- to define proper email use and restrictions (e.g., mass mailing, hoaxes, autoforwarding)
- to explain expected results of policy violations (1^{st}, 2^{nd}, 3^{rd}, etc)

(Note: Activity in any criteria can lead to criminal offenses.)

q. The authority for soliciting a social security number (SSN) is EO 939. The information below will be used to identify you and may be disclosed to law enforcement authorities for investigating or prosecuting violations. Disclosure of information is voluntary; however, failure to disclose information could result in denial of access to (*insert your organization*) information systems.

7. Acknowledgement. I have read the above requirements regarding use of (*insert your organization*) access systems. I understand my responsibilities regarding these systems and the information contained in them.

insert name here
Directorate/Division/Branch

insert date here
Date

insert name here
Last Name, First, MI

insert Rank/Grade and SSN here
Rank/Grade/ SSN

insert name here
Signature

insert phone number here
Phone Number

Figure B–1. Acceptable use policy—Continued